FireEye
SECURITY REIMAGINED

"Show Me" Cyber Security in Missouri

State Turns to FireEye to Protect Vital Citizen Data

CUSTOMER STORY

SECURITY REIMAGINED

CUSTOMER PROFILE

Missouri is a state located in the Midwestern United States with a population of 6 million citizens. Approximately 50,000 state employees in over 100+ locations around Missouri enable hundreds of various services for citizens, businesses, and visitors. The state comprises 114 counties with the largest metro areas being Kansas City and St. Louis.

"Cyber security is the state's number one priority, from an IT perspective, to ensure that our citizens' data remains secure and safe."

— **Michael Roling,** chief information security officer, State of Missouri

Like all U.S. states, Missouri maintains extensive information on its citizens, including birth and death records, taxes paid and owed, health information, property ownership, criminal records and more. If someone with malicious intent hacks into those records, the risk of identity theft and subsequent harm is considerable. So Missouri citizens are right to expect their state to "show me" — per the state's nickname — how well it secures those records.

"Cyber security is the state's number one priority from an IT perspective to ensure that our citizens' data remains secure and safe," said Michael Roling, Missouri's chief information security officer (CISO). Roling's job is to secure sensitive information on nearly six million Missouri citizens.

"WE DID NOT WANT TO BE THE NEXT VICTIM"

According to Roling, after witnessing very damaging cyber security breaches in other states, Missouri officials decided they "did not want to be the next victim" and needed to secure the state's IT systems before it suffered a major breach.

"We saw what was happening around us. We saw what that did to the trust between the citizens and the government," he said.

Roling, who's been Missouri's CISO for six years, said its cyber security profile before 2013 was limited, with just four staffers and otherwise finite resources, funding, tools and technology. Fortunately, he added, the state's executive and legislative branches were on board with enhancing security. One of the key partners the state chose to accomplish this was FireEye.

NX, EX, OTHER SERIES WORK AS ONE SYSTEM

Missouri began by acquiring FireEye® Network Security (NX Series) to secure the state's networks. That was followed by deploying FireEye® Email Security (EX Series). Many of the attacks on

> "Having (FireEye) technologies in place has reduced the number of incidents over time and … the amount of time that it takes my staff to investigate."
>
> — **Michael Roling,** chief information security officer, State of Missouri

Missouri's state networks came in the form of spear-phishing emails that secretly delivered malware. "When EX discovers malicious email, it provides the information to all of the other FireEye technologies to ensure maximum protection," Roling explained. The state then began using FireEye® File Content Security (FX Series) to scan file-sharing systems, FireEye® Malware Analysis (AX Series) for ad hoc malware forensics and FireEye® Endpoint Security (HX Series).

More recently, Missouri began deploying FireEye® Mobile Threat Prevention (MTP) technology to extend security to mobile devices that state employees are increasingly using, he said. MTP will also help the state manage security as the "Internet of Things" evolves.

"Those two areas are probably the issues that keep me up at night. It's about how we can ensure that business is conducted securely from a mobile standpoint, and then how we ensure that the Internet of Things is secure," said Roling.

FireEye security technology now protects as many as 50,000 endpoints throughout the state's network, including 40,000 endpoints over which the state has "direct authority," Roling explained. There are another 10,000 endpoints that some state agencies and departments have established on their own, but these operate on the larger state network and as such they enjoy the added protection of the FireEye NX Series.

"This is one of the coolest things about this from a geek perspective," Roling said, adding that the integration of email and network security was a key advantage FireEye offered over another vendor the state was considering.

BEING PROACTIVE VERSUS REACTIVE

Now that the FireEye deployment is complete, Roling said Missouri's cyber security profile is decidedly proactive instead of reactive.

With FireEye, his department is seeing new threat information that wasn't visible before. When an incident comes to their attention, they have the visibility and tools to resolve it. This kind of insight has significantly improved their security.

"Having the FireEye technologies in place has reduced the number of incidents over time and it has also reduced the amount of time that it takes my staff to resolve incidents," he said. "We quickly saw that when we adopted the HX endpoint solution. The time to resolve incidents shrank from around 110 hours to 5 hours or less, a decrease of more than 95%."

Not only has the FireEye deployment reduced the time to respond to cyber security incidents, it has also reduced the time an adversary may be on the network before the state discovers and removes it. These technologies have not only mitigated threats to the network but have freed up hundreds of staff hours per month, creating efficiencies within Roling's cyber security team, in IT and throughout the state government.

"PROOF OF CONCEPT" A CRITICAL STEP

When asked to provide advice to other states contemplating a cyber security project, Roling said he's mystified when organizations choose not to perform a "proof-of-concept" test before making the investment. Missouri made sure to do one and was impressed that the FireEye system was up and running in less than 30 minutes.

"FireEye is spending money in the right ways, particularly in research and development," he said. "At the end of the day, I want the best technology and the best solutions that can detect compromises and advanced malware."

What's more, deploying the FireEye technology within the state network has raised awareness about cyber security and threats, and not just within IT. Roling's group is now able to share cyber security intelligence with stakeholders throughout the state who can quickly see the value of the solution.

In short, FireEye has answered Missouri's demand to show how effectively it can secure critical IT resources for the good of its citizens.

"I'm very happy with our relationship with FireEye, from sales to support to engineering," said Roling. "They've all been phenomenal."

To learn more about FireEye, visit:
www.fireeye.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**